Department of Veterans Affairs
Washington, DC 20420

VA Directive 6214
Transmittal Sheet
March 15, 2002

INFORMATION TECHNOLOGY SECURITY CERTIFICATION AND ACCREDITATION PROGRAM

1. REASON FOR ISSUE: This directive prescribes the policies and responsibilities for the implementation of the Department of Veterans Affairs (VA) Information Technology Security Certification and Accreditation Program (ITSCAP).

2. SUMMARY OF CONTENTS. This document:

a. Establishes a uniform, standards-based policy for the certification and accreditation of VA information systems (formerly referred to as Automated Information Systems).

b. Defines a methodology that will be implemented throughout VA to ensure that VA information systems conform to applicable security requirements and will continue to maintain accreditation throughout the system life cycle.

c. Describes the responsibilities of the personnel involved in the certification and accreditation process.

3. RESPONSIBLE OFFICE: The Office of Cyber Security (045C), Office of the Assistant Secretary for Information and Technology, is responsible for the material contained in this directive.

4. RELATED HANDBOOK: VA Handbook 6214, VA Information Technology Security Certification and Accreditation Program (Pending).

5. RESCISSIONS: None.

CERTIFIED BY:

/s/
John A. Gauss
Assistant Secretary for Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
John A. Gauss
Assistant Secretary for Information and Technology

Distribution: RPC: 6001
FD

INFORMATION TECHNOLOGY SECURITY CERTIFICATION AND ACCREDITATION PROGRAM

1. **PURPOSE.** The Veterans Affairs Information Technology Security Certification and Accreditation Program (VA ITSCAP):

a. Establishes a standards-based uniform policy for the Certification and Accreditation (C&A) of VA Information Systems (ISs).

b. Provides mandatory, minimum security requirements for accreditation. Requirements that are more stringent may be necessary for selected systems based on an assessment of acceptable level of risk. Systems will be analyzed for proper and full implementation of the security requirements by assessing whether critical security features are implemented correctly and completely and that controls are commensurate with risk.

c. Provides a disciplined approach to managing information security consistent with processes used throughout the Federal Government and private sector. The VA ITSCAP process is based on the National Information Assurance Certification and Accreditation Process (NIACAP).

d. Integrates security into the VA business cycle. The VA ITSCAP has been designed to support the VA Strategic Management Plan and Capital Investment Process and provide a means for the information security staff to advise the program management staff. The process is oriented on business information and business process perspectives and not around technology or its vulnerabilities.

e. Utilizes a life cycle management approach to help Program Managers implement C&A.

f. Identifies roles and responsibilities for personnel involved in the C&A process.

2. POLICY.

a. **General**

(1) **Process**. VA ITSCAP will be used throughout VA to ensure ISs meet applicable security requirements, security controls are commensurate with risk, and maintain accreditation throughout the systems' life cycle. VA's ITSCAP complies with Federal guidance such as those published by the National Institute of Standards and Technology (NIST). The VA ITSCAP process is based on the NIACAP, with modifications for specific VA requirements. VA's ITSCAP is composed of seven objectives:

(a) Objective 1, Registration

(b) Objective 2, Acquisition

(c) Objective 3, Preparation

(d) Objective 4, Implementation and Testing

(e) Objective 5, Authorization

(f) Objective 6, System Maintenance

(g) Objective 7, System Closeout

(2) **Business Process**. C&A will be introduced into the business process of VA's ISs. The ITSCAP supports VA's Strategic Management Council (SMC) and Capital Investment Board (CIB).

(3) **Cost**. The VA Program Manager (PM) must include an ITSCAP funding line item in the program budget to ensure sufficient C&A funds are available.

(4) **System Registration**. All ISs must be registered with the Office of Cyber Security (045C). All organizations must verify and update the C&A status of their ISs with the Office of Cyber Security (045C) by October 1 of each year.

(5) **Security Requirements**. VA has developed operating system specific protection profiles to describe the functional and assurance requirements that ensure compliance with applicable laws and regulations. VA should use the requirements specified in VA Security Protection Profiles for Sensitive Level 1, Level 2, and Level 3 Information Systems as minimum security requirements wherever possible. VA may also use NIST guidance as well as protection profiles from National Information Assurance Partnership (NIAP), National Security Agency (NSA), and approved sources where VA profiles do not suffice.

(6) **System Interconnection Agreement (SIA)**. When ISs are interfaced, networked, or otherwise connected to another system (outside the accreditation boundary) an SIA is required. An SIA is a stand-alone document required for systems connecting to all other systems whether internal to VA or external. The SIA will address the accreditation requirements of each system involved, include a description of the system, information processed on the system, connections to other systems, and safeguards to be implemented before interfacing with the IS. The SIA will include a description of all protections afforded to connections that use the Internet. The SIA should designate the appropriate individual to resolve conflicts among the interfaced or networked systems and should be reviewed and approved by the ISO at that facility. All SIAs are to become an appendix to the System Security Security Authorization Agreement (SSAA).

(7) **Rules of Behavior.** Rules of behavior policies must be created and agreements signed by users prior to a user being given access to the system. Rules of behavior policies will become part of the SSAA documentation. The rules shall be based on the needs of the various users of the system. The security required by the rules shall be only as stringent as necessary to provide adequate security for information in the system. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the system.

(8) **Configuration Management**. Configuration management is an integral component of security management. Configuration management ensures that the system is continually assessed to determine the impact of changes to a certified and accredited system and system documentation is maintained and kept up to date. Change is ongoing as the system responds to the needs of the user and new technology is developed, but the impact of these changes on the system must be determined to ensure an appropriate security posture is maintained. As threats become more sophisticated or focused on a particular asset, safeguards must be strengthened or added to provide adequate protection. Therefore, configuration management must be implemented to maintain an acceptable level of residual risk.

(9) **Implementation Timetable for VA Systems.**

(a) **New System**. New systems must use the VA ITSCAP effective immediately. If another process has been started, the Office of Cyber Security will provide guidance to transition to VA ITSCAP.

(b) **Existing System**. Existing VA systems must be certified and accredited. The VA Office of Cyber Security will establish dates for these systems.

b. **Certification Initiation**. All VA general support systems and all major applications must be certified and accredited. Table 1 shows which VA objectives must be completed for each event described in OMB Circular A-130, Appendix III.

	Objective 1 Registration	**Objective 2 Acquisition**	**Objective 3 Preparation**	**Objective 4 Implementation & Testing**	**Objective 5 Authorization**	**Objective 6 System Maintenance**	**Objective 7 System Closeout**
New System	X	X	X	X	X	X	
Major Modification	X	X	X	X	X	X	
Change In Time	X		X	X	X	X	
Initial Certification	X		X	X	X	X	
System Closeout							X

Table 1

(1) **New System**. A new IS is required to follow VA ITSCAP prior to acquisition. All objectives apply except “System Closeout” (Objective 7) for a new system.

(2) **Major Modification**. Major changes to an IS, separately accredited major application, their associated environment that affects the accredited security architecture, or significant changes to the prescribed security requirements require a new risk assessment and re-accreditation. Major changes include: an increase in the sensitivity/criticality of a

system, an increase in threat level, policy change, a change in operating system (base platform), a change to security relevant software, a change to hardware that could affect the security architecture, an increase in interconnection with other systems outside the accreditation boundary, or significant changes in the security requirements that apply to the system. All objectives except “System Closeout” (Objectives 1-6) must be completed for the re-accreditation of systems with major modifications.

(3) **Change In Time**. At a minimum, VA IS or separately accredited major applications must be re-accredited every three years. Systems, or portions of systems, with significant residual risk should be re-accredited on a shorter cycle than the usual 3 years. A system with significant residual risk is a system that processes mission critical information that is directly accessed or altered by veterans or the public. The Designated Approving Authority (DAA) may also designate systems requiring more frequent security accreditation. All objectives except “Acquisitions” (Objective 2) and “System Closeout” (Objective 7) are generally accomplished on systems undergoing their cyclic re-accreditation.

(4) **Initial Certification**. Existing systems that have not been previously certified must follow VA’s ITSCAP. All objectives except “Acquisitions” (Objective 2) and “System Closeout” (Objective 7) are generally accomplished on existing systems undergoing an initial accreditation.

(5) **System Closeout**. When an IS or major application has been targeted for closeout, “System Closeout” (Objective 7) must be completed.

c. **ITSCAP Roles and Responsibilities**

(1) **Designated Approving Authority (DAA)**. The VA DAA is the VA’s Chief Information Officer (CIO). This individual has the authority to formally accredit a system from an information security perspective. See paragraphs 2e and 2f for the definition of the different accreditation choices and decisions that may be made. The VA DAA is responsible for ensuring the C&A program is properly funded. The VA CIO may delegate the DAA responsibilities, in writing, but will retain the final approving authority for all accreditations within VA. The VA DAA must approve all accreditations.

(2) **Registration Agent (RA)**. The RA is the Office of Cyber Security. This is the organization that manages system registration and certification status and collects electronic copies of ITSCAP documents.

(3) **Certification Agent (CA)**. The VA CA is the VA Information Security Officer (ISO) located within the Office of Cyber Security. This individual is responsible for advising the VA DAA on security practices and signing the official certification recommendation to the VA DAA. A delegated DAA may delegate a CA, in writing. Delegated CAs must be independent from the organization responsible for system development or operation. Organizational independence of the CA ensures the most objective information for the DAA to make an accreditation decision.

(4) **Certification Team**. The Certification Team is responsible for making a technical judgment of the system’s compliance with stated requirements, identifying and assessing the

risks associated with operating the system, coordinating the certification activities, recommending additional security measures, and consolidating the final ITSCAP documents. The Certification Team must be independent from the organization responsible for the system development or operation. For example, a Certification Team comprised of VHA employees may certify a system within VHA, if the team members are not involved in the system development or operation of the system in question.

(5) **Program Manager (PM)**. The PM is the official responsible and accountable for coordinating the business aspects of managing the system from initial concept, through development, to implementation and system closeout. The PM must add an ITSCAP funding line item to the program budget to ensure C&A funds are available. Different individuals may assume the PM role during different phases of the system life cycle. The PM will determine the sensitivity of information in the system and appropriate protection to be taken.

(6) **User Representative**. The User Representative is the individual or organization that represents the user or user community in the definition of IS requirements, development or implementation of the system, and system operations.

(7) **Information Security Officer (ISO)**. The ISO is typically responsible to the DAA for managing the security program to ensure appropriate security is maintained throughout a system's life cycle, from design through disposal.

(8) **Systems Security Manager (SSM)**. The SSM is the individual with the technical ability and responsibility to implement IS security configuration controls, report security incidents, and implement security changes for specific systems.

(9) **Information Owner**. The information owner determines the sensitivity of information in the system and the appropriate protections to be afforded. The information owner also authorizes who has access to the system and what functions they are permitted to perform. These tasks may be delegated to the PM acting as the information custodian.

d. **VA ITSCAP Process Description**

(1) **Process Scope**. ITSCAP is a structured process that provides a uniform, standards-based, and repeatable approach using a disciplined body of information security methods and rules. VA's ITSCAP will be used to accredit VA's IS regardless of its stage in the system life cycle. The process is designed to certify that the IS meet documented security requirements and will continue to maintain the accreditation throughout the life cycle. VA's ITSCAP is composed of seven objectives.

(a) **VA Objective 1, Registration**. Applies to all events that initiate accreditation. The registration objective is focused on understanding the business case, environment, threats, and system architecture to determine the security requirements and level of effort necessary to achieve accreditation. Individuals and organizations involved in the C&A process must be identified. Participants of this objective must agree on the security requirements, accreditation boundary, schedule, level of effort, and resources required. They will collect and review security documentation, prepare the mission description and system identification and conduct a certification requirements review. A preliminary risk assessment will be conducted to identify risks associated with the system early in the C&A process. The registration objective is started when the conceptual design of an IS is initiated, major change to an existing system is required, or when initial accreditation or re-accreditation of an existing system is due. The system registration is submitted to the RA and must include the names of the individuals assigned to the roles associated with the C&A process, contact information, and a well-defined description of the system or application. An approved System Security Authorization Agreement (SSAA), described in subparagraph 2, is the final product of Objective 1. The CA approves the Objective 1 SSAA. VA Objective 1, Registration is the same as NIACAP Phase 1, Definition, with the addition of a preliminary risk assessment.

(b) **VA Objective 2, Acquisition**. Applies to both new systems and major modifications of systems. The PM is responsible for ensuring that security requirements are defined. The CA advises the DAA and CIB (Capital Investment Board) if the risks associated with the IS are reasonably identified for the system mission and environment, if the security requirements adequately address those risks, and if additional measures are necessary to mitigate risk. After a Statement of Work (SOW) has been prepared, the CA reviews the SOW to ensure the security requirements defined in the SSAA and the expected risks have been adequately addressed. After a Request for Proposal, with the SOW, has been issued and proposals have been received, the CA advises the PM if the proposals or security targets meet the defined security requirements and adequately address the risk associated with the IS. In the event that proposed security targets do not adequately meet the requirements, the CA should advise the DAA and CIB about implementing safeguards that may reduce residual risk more fully. This objective does not apply to existing systems that are conducting their initial accreditation or to accredited systems that must be re-accredited due to changes in time. VA Objective 2, Acquisition takes place between NIACAP Phases 1 and 2 and is intended to support the requirements of the Clinger-Cohen Act.

(c) **VA Objective 3, Preparation**. Applies to events that initiate accreditation. This objective verifies the system's compliance with the information in the SSAA. The purpose of this objective is to ensure that the fully integrated system will be ready for testing. The Certification Team conducts analyses of the system architecture, software design, network connections, integrity of integrated products, and life cycle management. The Certification Team prepares test plans and procedures to be used during Objective 4, Implementation and Testing. The team conducts an initial vulnerability assessment on the proposed implementation and identifies the potential risks. VA Objective 3, Preparation is the same as NIACAP Phase 2, Validation.

(d) **VA Objective 4, Implementation and Testing**. Implementation starts after the initial risk assessment has been done. A Certification Plan must be in effect, and the System Security Plan and Rules of Behavior (including signed user agreements for each user of the system) must have been developed, updated and reviewed. A security evaluation by the PM has certified that the security controls are in place and have been validated as adequate, appropriate for the system, and operating as intended prior to testing. Testing validates compliance of the fully integrated system with the security policy and requirements stated in the SSAA. The purpose of this objective is to produce the required evidence to support the CA’s recommendation to the DAA. This is accomplished by conducting a system test and evaluation, a penetration test, communications security evaluation, system management analysis, site evaluation, contingency plan evaluation, and risk analysis evaluation. After the testing has been completed, the Certification Team conducts an updated risk assessment. The Team consolidates the security analyses into the SSAA and prepares a recommendation for the CA and CIB. The recommendation is submitted to the CA to review and forward to the DAA. VA Objective 4, Implementation and Testing is a combination of NIACAP Phase 2, Verification and Phase 3, Validation.

(e) **VA Objective 5, Authorization.** Begins after the completion of security testing. The authorization to process is the formal acceptance, by a non-security management official (the DAA), of the residual risks associated with the system after controls have been installed and tested. Pursuant to NIST Guidance 800-18 *Guide for Developing Security Plans for Information Technology Systems*, authorization is not a decision to be made by the security staff. The security staff has the responsibility to direct, perform, or monitor security tasks for the system, and to make an authorization recommendation to the DAA. The DAA will then decide, based on the evidence presented by the security staff, whether the residual risks have been minimized to the point where they are acceptable. The DAA will then issue a system accreditation letter. The accreditation letter must be included in the SSAA and contain the date of authorization, as well as the name and title of the DAA.

(f) **VA Objective 6, System Maintenance**. Starts after the system has been certified and accredited for operation. System operation objectives include those activities necessary for the continuing operation of the accredited IS in its environment, and to address the changing threats and small-scale changes a system faces throughout its life cycle. The goal of this objective is to ensure secure system management, operation and maintenance to preserve an acceptable level of residual risk. VA Objective 6, System Maintenance, is the same as NIACAP Phase 4, Post Accreditation.

(g) **VA Objective 7, System Closeout**. Covers the decommissioning of a system or major application. The purpose of this objective is to securely closeout a system. Actions include wiping disks and disposing of or reusing any IS components. The CA evaluates the decommissioning policies and advises the PM if the policies are adequate, if appropriate procedures have been implemented, and recommends additional procedures if the existing procedures are inadequate. The PM must contact the RA and report the change in system status. If necessary, a Certification Team prepares and conducts tests on the system to verify that the system is ready for disposal or reuse. VA Objective 7, System Closeout, is not in the NIACAP, but is included to address specific VA requirements.

(2) **System Security Authorization Agreement Description**. The SSAA is intended to consolidate security related documentation into one document. This eliminates the redundancy and potential confusion caused by using multiple documents to describe the system. The SSAA is also a formal agreement between the DAA, CA, Certification Team, User Representative, and PM. The SSAA is used throughout the C&A process to guide actions, document decisions, specify security requirements, document certification tailoring and level of effort, identify possible solutions, and maintain operational system security. The SSAA has the following characteristics:

(a) Compatible with OMB Circular A-130 and NIST requirements.

(b) Includes a NIST recommended System Security Plan (See NIST Special Publication 800-18, “Guide for Developing Security Plans for Information Technology Systems.” The system security plan purpose is to provide an overview of the security requirements of the system and describe the controls in place (or planned) for meeting those requirements.

(c) Establishes the accreditation boundary of the system.

(d) Documents the formal agreement between the DAA, CA, Certification Team, PM, and User Representative.

(e) Documents the C&A results and defines the residual risks.

(f) Contains the letter authorizing approval to operate.

(g) The physical characteristics of the SSAA will depend on the certification complexity and organizational requirements. All SSAAs will contain a system security plan and contingency plan. The goal is to produce an SSAA that contains all agreements and will be the basis of agreement throughout the system's life cycle. The SSAA can be tailored to incorporate other documents as appendices or by reference.

(h) The DAA, CA, Certification Team, PM, and User Representative have the authority to tailor the SSAA to meet the characteristics of the IS, operational requirements, security policy, and prudent risk management. The SSAA is flexible enough to permit adjustment throughout the system's life cycle as conditions warrant. New requirements may emerge from design necessities, existing requirements may need to be modified, or the DAA's overall view of acceptable risk may change. When that occurs, the SSAA is updated to accommodate the new components. The SSAA is developed in Objective 1 and updated in each subsequent objective as the system development progresses and new information becomes available. The completed SSAA contains those items that must be agreed to by the DAA, CA, Certification Team, PM, and User Representative. The organizations supporting the C&A effort must understand each of these essential items.

(i) The SSAA must identify all costs relevant to the C&A process. The PM is the responsible official that must add an ITSCAP funding line item to the program budget to ensure adequate funds are available. Funding must cover any contractor support, travel, or test tool costs associated with the C&A process.

(j) If a system security plan has already been prepared according to NIST guidance, it may be incorporated in and appropriately supplemented to produce an SSAA.

e. **Accreditation Choices**

(1) **Site**. A site accreditation evaluates the applications and systems at a specific physical location.

(2) **System**. A system accreditation evaluates a general support system or major application.

(3) **Type**. A type accreditation evaluates an application or system that is distributed to a number of different locations.

f. **Accreditation Decisions**

(1) **Interim Approval to Operate**. An Interim Approval to Operate (IATO) may be granted for up to six months by the DAA, if the system has a preliminary risk assessment, contingency plan, draft SSAA, and a plan for when the C&A will be conducted and completed. The IATO is granted to complete the remaining certification requirements and expeditiously mitigate deficiencies. After successful completion of the remaining requirements and mitigation of deficiencies identified in the IATO, the SSAA should be re-evaluated and the system's accreditation status may be upgraded accordingly.

(2) **Conditional Approval to Operate**. The DAA may grant a Conditional Approval to Operate (CATO) for up to one year for systems that have completed a certification but contained too significant an operational risk to be accredited. This may range from a single very high-risk item to several lower-risk items that, in combination, pose too great an operational risk. The CATO is granted on the condition that a program has been developed and implemented to reduce the residual risks identified with the system. After successful implementation of added safeguards that reduce the risks, the SSAA should be re-evaluated and the system's accreditation status may be upgraded accordingly.

(3) **Full Accreditation**. Full accreditation is a formal declaration by a DAA that an IS is approved to operate in a particular security mode, using a prescribed set of safeguards, to attain an acceptable level of risk. A full accreditation is valid for no more than three years or until a major change affects the system, whichever comes first.

(4) **Accreditation Denied**. If the system does not satisfy the security requirements and the residual risks place the system operation or information in jeopardy then accreditation can be denied and the system is not authorized to process.

3. RESPONSIBILITIES

a. **VA Chief Information Officer (CIO)**. The VA Chief Information Officer (CIO) is the DAA.

b. **VA Information Security Officer (VAISO)**. VA's Information Security Officer (ISO) is the Associate Deputy Assistant Secretary for Cyber Security and is the CA for VA.

c. **Under Secretaries and Assistant Secretaries**. The Under and Assistant Secretaries are responsible for overseeing the C&A of the general support systems and major applications for which they are responsible. They must ensure that funding and resources are adequate to accredit information systems.

d. **VA Office of Cyber Security (OCS)**. The VA Office of Cyber Security (OCS) is the VA RA. OCS will monitor VA C&A efforts, provide centralized support to aid VA officials in their efforts to accredit general support systems and major application, advises the CIO on the appropriate delegation of authority, and establish security standards and guidelines for components and systems.

4. REFERENCES

a. ISO 15408, Common Criteria for Information Technology Security Evaluation, Version 2.1, September 19, 2000.

b. National Institute of Standards and Technology (NIST) Publications and Guidance.

c. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), April 2000.

d. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, National Information Systems Security (INFOSEC) Glossary, September 2000.

e. Office of Management and Budget (OMB) Memorandum M-01-08, “Guidance on Implementing the Government Information Security Reform Act,” January 16, 2001.

f. Office of Management and Budget (OMB) Circular No. A-130, Transmittal 4, November 2000, “Management of Federal Information Resources”.

g. Public Law 100-235, Computer Security Act of 1987, January 8, 1988.

h. Public Law 104-106, Clinger-Cohen Act of 1996, August 8, 1996.

i. Public Law 106-398, FY 2001 Defense Authorization Act, Title X, subtitle G, Government Information Security Reform Act, October 30, 2000.

j. VA Directive 6210, Automated Information Systems Security, January 30, 1997.

k. VA Handbook 6210, Automated Information Systems Security, January 30, 1997.

5. DEFINITIONS

a. **Accountability**. Process of tracing IS activities to a responsible source. Accountability includes authenticity and non-repudiation.

b. **Accreditation**. A formal declaration by a DAA that an IS is approved to operate in a particular security mode at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

c. **Architecture**. The configuration of any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment and services, including support services and related resources.

d. **Automated Information System (AIS)**. See Information System (IS).

e. **Availability**. Timely, reliable access to data and information services for authorized users.

f. **Certification**. Comprehensive evaluation of the technical and non-technical security features of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

g. **Certification and Accreditation (C&A) Boundary**. Encompasses all the components of the system that are to be accredited by the DAA and excludes a separately accredited system, to which the system is connected.

h. **Confidentiality**. Assurance that information is not disclosed to unauthorized persons, processes, or devices.

i. **General Support System**. Interconnected set of information resources under the same direct management control which share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a LAN including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. (OMB Circular A-130, Appendix III)

j. **Information System (IS)**. The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. An IS can be a general support system or a major application.

k. **Integrity**. Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. In a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

l. **Major Application**. An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the system in which they operate. (OMB Circular A-130, Appendix III)

m. **Risk Assessment**. Process of analyzing threats to and vulnerabilities of an IS and the potential impact the loss of information or capabilities of a system would have on security. The resulting analysis is used as a basis for identifying appropriate and cost-effective safeguards.

n. **Security**. Measures and controls that ensure confidentiality, integrity, availability, and accountability of the information processed and stored by a computer.

o. **System Security Authorization Agreement (SSAA)**. A formal agreement among the DAA(s), Certification Agent, Certification Team, User Representative, and Program Manager. It is used throughout the VA ITSCAP to guide actions, and to document decisions, security requirements, certification tailoring and level of effort, certification results, Certification Agent's recommendation, and the DAAs' approval to operate.

p. **Threat**. Any circumstance or event with the potential to harm an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

q. **User**. Person or process authorized to access an IS.

r. **Vulnerability**. Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited.